(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/05476 A1

(51) International Patent Classification[7]: H04L 9/00, H04K 9/00

(21) International Application Number: PCT/IL01/00620

(22) International Filing Date: 6 July 2001 (06.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/611,297 6 July 2000 (06.07.2000) US

(71) Applicant *(for all designated States except US)*: **VERIFOX TECHNOLOGIES LTD.** [IL/IL]; Geneo Street 1/4, 91000 Jerusalem (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COHEN, Rami** [IL/IL]; Geneo Street 1/4, 91000 Jerusalem (IL). **KALISH, Igal** [IL/IL]; Haofarim Street 8, 85025 Metar (IL).

(74) Agent: **FRIEDMAN, Mark, M.**; Beit Samueloff, Haomanim Street 7, 67897 Tel Aviv (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/05476 A1

(54) Title: AUTOMATIC AUTHENTICATION SYSTEM THAT CROSS-VERIFIES DIGITAL IDENTITIES

(57) Abstract: An authentication system including an active smart-key (20) for automatically cross verifying all partners involved in communicating or transacting online, using any Internet enable device (15) or system. This invention enables users to communicate and transact from any Internet enabled device, in a secure and easy to use way, without transferring any personal details between the user and the merchant or source (10). All personal information is given over when registering as user, and is not used by any third parties. The system verifies all the relevant users every time a new page or device is used, ensuring a constantly authenticated and highly private information communication experience online.

AUTOMATIC AUTHENTICATION SYSTEM THAT CROSS-VERIFIES DIGITAL IDENTITIES

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a secure automatic authentication system for cross-verifying digital identities of transaction or information sharing partners, without a need for transferring personal information.

One of the major obstacles restraining the boom in Internet commerce and highly sensitive information sharing is security concerns. Users are expected to provide personal information when transacting a sale or initiating sensitive communication, and are rightly concerned that any personal information provided can be given over to the wrong hands and used in unauthorized ways.

Various attempts have been made to secure online transactions and communications. The following table illustrates competing strategies and their pros and cons. Verifox represents the technology of the current invention.

The solution	Mobility	Security Level	User friendliness/Simplicity	Psychological Factor	Dedicated Interface
Credit Cards	+	--	++	--	+
Smart Cards	-+	-	++	-	-
Bio-metrics	-+	--	++	++	--
Software	-	+	+	--	+
ISP	-	-	++	+	+
Token Based	-+	+	+	+	-
Verifox	+	++	++	++	-

Most known Internet security systems tend to protect the identity of the purchaser by decoding and encoding personal information provided during the transaction process. However this information is always available to potential hackers, and is also vulnerable to unauthorized usage from the side of the merchant.

There is thus a widely recognized need for, and it would be highly advantageous to have, a system where both communicating peers are able to be continually cross verified, without requiring a transfer of personal information, and

where private information is not stored or channeled to trading partners. It would also be beneficial to have a system where the user can identify themselves using any type of Internet enabled device or system, and where unauthorized usage of the system would lead to rapid disabling of the system.

The present invention facilitates secure online transactions and communications by verifying all the involved parties on a dynamic basis. For example, the current invention is able to verify both the buyer and seller, on every page where a possible transaction or sensitive exchange of information is required, without the need to transfer personal information between them. Users of the current invention may possibly execute secure Internet transactions from any Internet enable device that the smart-key can connect to, with no need to download any specific software or install any specific hardware. The key will connect to all major hardware communication components, such as USB's, RS232 etc., as well alternative information transfer means such as radio waves, infra red etc. The key will have an internal computer that is able to receive, store, process and send the necessary information in order to ensure secure, cross-verified communications and transactions.

SUMMARY OF THE INVENTION

According to the present invention there is provided a system for automatically cross verifying all partners involved in transactions and information transfer using the Internet, with any Internet enabled systems or devices, comprising:

i) A smart-key authentication device with software programs based on trap door algorithms and hash functions for the smart key that are able to generate keyed message digests, encode and decode binary data. This key will be used for storing, processing and communicating encrypted information;

ii) A Web server with a secret key database for storing, decrypting, processing and communicating relevant information, and executing transactions;

iii) Client devices or systems, such as cellular phones, PDAs, desktop computers and any other Internet enabled computing devices;

iv) Websites of vendors, financial institutions, information providers etc with software that will provide the interface for users to enter information into the system.

The present invention is that of a secure automatic authentication system for cross-verifying digital identities of information sharing partners, without a need for transferring personal information. The system is comprised of a portable device, called a smart-key, software programs for the smart-key, a central database and client software for users. The smart-key is a mini-computer that can store, process and communicate information, such as personal identification numbers (PIN), contact and identity information, bank and credit card details, personal preferences, codes and more. The smart-key typically contains the digital identities of the user and the set of communication peers (communication partners including people, companies and Websites on the users' contact or trade list). The digital identities are encrypted, and the key can both receive and broadcast encoded and decoded information in order to authenticate a communication peer, as well as provide the peer with the means of authenticating the user. The invention stores all the private information on the key, and enables secure communications using only PIN codes etc., so that no other personal information needs to be transferred over the Internet. Furthermore the identity of both users communicating are re-authenticated each time a new page or device is accessed. In this way users can conduct extremely secure, automatically cross-authenticated transactions and communications using multiple Internet enabled devices. The current invention uses current communication standards such as USB, RS232, infrared RF and other electromagnetic technologies to communicate with PC's, ATM's, PDA's, mobile phones or any other similarly equipped devices.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 illustrates the essential components of the key security system according to the present invention.

FIGURE 2 is a flow chart describing a typical user session of the key security system according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is of a system for automatically cross verifying all partners involved in transferring information or executing transactions online, using any Internet enabled system or device.

The principles and operations of such a system according to the present invention may be better understood with reference to the drawings and the accompanying description, wherein:

FIGURE 1 illustrates the essential elements of the key security system according to the current invention. The following describes one of many possible embodiments of the present system. The system, however, is continuously being changed to follow changing market requirements and the continuously developing software environment.

1. The current invention, or Verifox Authentication System, executes on three processors:

The three processors are a) The authentication server **10** b) the client device or workstation **15**, and the c) the Verifox key or authentication device **20.**
The execution environments of each of these processors are specified in the following sections.

2. Execution Environments

2.1 Authentication Server Environment

The authentication server **5** according to the present configuration has the following specifications:

a) The operating system is RedHat Linux 5.1
b) The HTTP server is apache_1.3.12 or apache_1.3.12+ssl_1.39
c) The SSL encryption is provided by openssl-0.9.4
d) The HTTP server is built with php-3.0.12
e) PHP is built with mhash-0.7.0
f) For the Verifox project we have added an extension to mhash-0.7.0 that provides keyed SHA1 hashing.
g) The database **11** is msql-2.0.10.1

h) Current compatible browser software includes Windows 2000, Netscape Navigator 4.x or Microsoft Internet Explorer 5.

2.2 Client Side Environment

The client environment **15** is a PC running Microsoft Windows 98 or Microsoft Windows 2000, Netscape Navigator 4.7 or Microsoft Internet Explorer 5.

2.3 Key Environment

The key environment **20** is currently a PC running RedHat 6.1. The planned environment is ScanLogic or any other USB processor.

3. Executable Files and Programming Languages

3.1 Server Executables

The authentication server has a series of HTML pages that contain embedded PHP code. The PHP code performs:

a) database access functions

b) random number generation

c) SHA1 hash computation

d) client authentication by means of hash comparisons

The HTML pages serve the client:

a) forms for data entry

b) a Java applet or ActiveX component **17** for accessing the USB port for communication with the key

c) Javascript or ActiveX glue routines for transferring parameters to and from the applet

d) graphic content in the form of GIF or JPG files

Currently the HTML pages contain the HTML code, PHP code and Javascript code. It would be better to separate the Javascript into a separate .js file since the Javascript code is identical for all server HTML pages.

The Java applet is compiled using the JDK1.8 javac compiler from Sun Microsystems. In the current implementation the applet is packaged in a

digitally signed jar file for use with a Netscape Navigator client.

3.2 The Client Executables

The client environment executables are the HTML pages that the client browser receives from the authentication server and the Java applet or activeX component that the client uses to communicate with the key using a USB.

The client browser must support execution of Java applets from an external JRE.

3.3 The Key Executables

The key executes compiled and linked ANSI C code that performs hashing hashing functions. There is one executable file.

4. Development Environment

The development environment includes:

1. ANSI C development
2. PHP development
3. Java development
4. HTML and Javascript development
5. Java code signing

These environments are described in the following paragraphs.

4.1 ANSI C Development

The keyed SHA1 hash extensions to mhash-0.7.0 are developed in ANSI C on the RedHat Linux 5.1 authentication server using the GPL licensed GNU C compiler version 2.7.2.3.

The mhash-0.7.0 stock build environment was modified slightly to cause it to build and install the extensions.

The key code has been developed on a RedHat Linux 6.2 workstation using GPL licensed GNU C compiler version egcs-2.91.66 19990314/Linux (egcs-1.1.2 release).

A custom makefile in GNU Make version 3.77 syntax was developed to build the key object files and the key executable.

The C debugger, GNU gdb 4.18, was used in debugging and testing the key code.

4.2 PHP Development

The PHP development does not require any special development environment other than a text editor.

4.3 Java Development

The Java development does not require any special development environment other that a text editor and the javac compiler. Testing the applet requires the ability to upload the applet class files to an HTTP server and then execute them using a browser.

4.4 HTML and Javascript Development

The HTML and Javascript development requires only a text editor for the code development. The testing requires uploading the HTML pages to an HTTP server and then rendering the pages using a browser on a client machine.

4.5 Java Code Signing

The Java applet code signing requires a code signing tool and code signing cryptographic certificate. We tested the applet first using the javakey code signing tool provided with JDK1.8 and certificates that we generated ourselves using javakey. This code signing enables execution of the applet using appletviewer or the HotJava browser.

We subsequently modified the applet to use the Netscape security classes and signed the applet using the Netscape code signing tool and a temporary code signing certificate good for 15 days provided by Netscape.

All of the applet signing tools execute in the Microsoft Windows environment. We developed several simple batch files to automate process of signing the applets.

5. Protocols

The Verifox Authentication System contains four distinct communication

protocols:

1. Key I/O protocol
2. USB port protocol
3. Javascript to Java applet protocol
4. Authentication protocol

5.1 Key I/O protocol

The key I/O protocol is currently a trivial asynchronous bufferred read/write protocol over RS232. To implement the key in firmware requires replacing this protocol with a semaphore protected read/write scheme since the firmware environment does not provide I/O buffering.

5.2 USB Port Protocol

The USB port protocol is a simple asynchronous read/write protocol that is currently implemented using a proprietary system driver communicating with a USB hardware device.

5.3 JavaScript to Java Apple Protocol

The Javascript to Java applet protocol is a trivial, one-to-one pair of function calls. One function passes a string to the applet. The other function passes a string to the applet and returns a string from the applet. This interface will be simplified to consist of only a single Javascript function that passes a string to the Java applet and returns a string from the applet.

5.4 Authentication Protocol

The authentication protocol is the message protocol between the authentication server, the client browser and the key that enables the user to perform secure authenticated transactions. This protocol is currently under development.

A demo version of the protocol is provided in the current implementation. The smart key authentication device **30** of the current invention is a mobile physical device (or possibly a hardware implant or software-implanted device) that may be in various physical forms. It will be able to access various computing and communication devices, by any mechanism that can connect it into one of the

device's sockets (or any other type of information entry possibility, such as Bluetooth, infra red etc.), or by a hardware implant into any system or device. This key may be customized according to the needs of the key suppliers, for example the various banks, consumer organizations and financial institutions. The key will be more than a smart card, it will have memory storage and transfer facilities, like a smart card, but in addition to this will have processing ability. In order to achieve this the key will be programmed with a trap door algorithm and a hash function, for permitting one-way function calculations. These programs can be adapted to a variety of hardware forms, The key includes a multiple layer programming for various applications, allowing the key to be easily adapted to the requirements of the particular hardware and software being used by a licensed agency

Transactions using the current invention can take place between transactional partners, or peers, using any Internet enabled devices, such as PCs, PDAs or mobile phones. The smart key according the current invention will be compatible with almost all of these devices. Following are the key principles of operation of the Verifox Authentication Key, according to the current invention:

1. The Key stores a secret consisting of binary data that represents the identity of the Key owner
2. The Key stores a set of secrets consisting of binary data that represent the entities with which the owner of the Key is willing to communicate
3. The Key stores a set of names, each one associated with one of the secrets
4. The Key has a set of programs for generating keyed message digests
5. The Key stores a set of names, each one associated with one of the message digest programs
6. The Key has a set of programs each of which can encode and decode binary data to or from a particular type of data format
7. The Key stores the secrets, names and programs in an encrypted format
8. The Key can accept a personal identification number (PIN) that enables its operation by decrypting the secrets, names and programs
9. The Key has a feature that permanently disables the Key if more than a predefined number of incorrect PIN's are accepted

10. The Key can receive a message consisting of a data format type, the name of a secret, a message digest program name, a message digest and a set of data, and can compute the message digest of the set of data using the named secret and the named program

11. The Key can compare the message digest that it received with the message digest that it computes and can store the result of the comparison

12. The Key can receive a message consisting of a data format type, the name of a secret, a message digest program name and a set of data, and can output the message digest of the data in the received format type

13. The output of the Key can be controlled according to the result of the message digest comparison

14. The Key has a proprietary interface over the USB bus

FIGURE 2 illustrates a prime example of the usage of the current invention, in the case of an online transaction. Any user of the current invention initially registers and subscribes via the site or any participating financial institution. Upon registration, all relevant personal and financial data is given over by the user or merchant. Each potential financial transaction type, for example between the user and a chosen merchant, is programmed as a single digital key that is known by both sides. In this way any future communication or transaction between the user and the merchant (referred to as a peer) will have a pre-defined identity unique to these two partners.

The registered user starts **30 (FIG 2a)** the buying or information accessing process from an Internet access appliance some type of navigational software, such as a Web browser **31** operating on a personal computer to access an Internet commerce site such as an online store or bank. The user specifies a preferred transaction using the forms or transaction pages **32** that the commercial site provides.

At this stage the user can decide to proceed as usual, entering credit card details etc., or to proceed with executing the transaction using the current invention. In order to complete the transaction the user uses a form or page provided by the commercial site to indicate that the user desires to authenticate the transaction using the Verifox Authentication System. The enabling feature for this to occur will be an

icon or textual reference to Verifox (the current invention), such as an applet. Typically this is a program written in the Java programming language (a Java Applet) or in ActiveX. Clicking upon this link will connect the user to the Verifox server. When a site has it own Verifox servers that includes its clients database, for example a bank, commercial or professional organization etc., the negotiations are as described between the client and the organization. But when a random transaction is being made with a foreign client there are no negotiations between the merchant and the client. In that case, the verification and negotiations are between the merchant/service supplier and the Verifox server, and in a totally separate action between the client and the Verifox server. When both of them have been authenticated the deal is approved.

Once connected to the Verifox server, a simple form requesting the user to identify him or herself to the commercial site using a one-time non-negotiable instrument such as a simple user name. This instrument is not a credit card number, social security number or other instrument that can be used by anyone for any other purpose than for identification to the commercial site. The commercial site verifies that it has a record for the user.

The commercial site server generates a random sequence of several hundred letters and generates a cryptographic signature of this sequence using a secret number, a copy of which is also stored in the Verifox key that the user possesses.

The commercial site saves the random sequence of letters in the user's record in its database. The commercial site sends a message to the user's access appliance containing the name of the commercial site, the random sequence of letters and the cryptographic signature. The user's access appliance receives the message from the commercial site. The user's access appliance uses a program that it receives from the commercial site in one of the pages that it downloads from the site to prompt the user to attach the Verifox key **34** to the appliance and to enter a personal identification number (PIN) **35**. The user then types in their PIN **36 (FIG 2b)**.

The browser then sends the personal identification number to the key **37**. The key verifies that the personal identification number is correct **38**. If the personal identification number is not correct the key returns an error message and maintains a

count of the number of sequential incorrect access attempts **39**. If the personal identification number is not correct the access appliance prompts the user to re-enter the number.

The access appliance sends the re-entered number to the key. If the count of the number of sequential incorrect accesses reaches a predefined number, such as three, then the key permanently disables itself and is no longer usable **40**.

If the personal identification number is correct **41**, the key sends a message to the access appliance to inform it that the key is activated **42 (FIG 2c)**. When the access appliance receives the message that the key is activated it sends the message containing the commercial site identifier, the random sequence of letters and the cryptographic signature that it received from the commercial site to the key.

The key stores the cryptographic signature in a buffer for later use. The key retrieves the commercial site's secret number from its internal memory that is associated with the commercial site name that it received in the message from the access appliance. The key regenerates the commercial site's cryptographic signature of the random sequence of letters contained in the message received from the access appliance using its copy of the commercial site's secret number.

The key compares the cryptographic signature that it received in the message from the access appliance with the cryptographic signature that it generated independently. If the signatures do not match, the key sends a message to the access appliance that indicates that the commercial site message could not be authenticated. The key cannot perform any other function until it receives a message from a site that it can authenticate. The key maintains a count of consecutive failures to authenticate commercial sites. If there are more than a predefined number of consecutive failures the key disables itself permanently.

If the signatures match, the browser instructs the key to sign the transaction docket with the user' s digital signature **51 (FIG 2d)**. The key subsequently generates a cryptographic signature of the random letters received from the commercial site using the user's secret number that is stored in the key, a copy of which is contained in the user's record on the commercial site. The signed docket is returned to the browser **52,**

indicating to the access appliance that the key has successfully authenticated the server message. The access appliance sends the user's signature of the random message to the commercial Website 53.

A similar process happens on the side of the Website of the commercial entity. The Website generates the cryptographic signature of the random letters that was previously sent to the user's access appliance and stored in the user's record, using its copy of the user's secret number that it has stored in the user's record.

If the cryptographic signature that the commercial site received from the access appliance does not match the cryptographic signature that the commercial site generated using the user's secret number, then the user is not authenticated and the commercial site discards the transaction. If the cryptographic signature of that the commercial site received from the access appliance matches the cryptographic signature that the commercial site generated using the user's secret number, then the user is authenticated to the server.

The server generates a new random sequence of letters and stores them in the user's record. The commercial site generates a cryptographic signature of the new sequence of random letters and a transaction docket using its secret number. The commercial site sends the transaction docket 43 (FIG 2c) and the new random letter and the cryptographic signature to the user's access appliance.

The access appliance displays the transaction docket 43 to the user and prompts the user to authenticate the transaction docket 43 and thereby complete the transaction. The user indicates his or her desire to authenticate the transaction by clicking on a button. The access application sends the transaction document, the random letters and the commercial site's cryptographic signature to the key. The key stores the cryptographic signature in a buffer for later use. The key retrieves the commercial site's secret number from its internal memory that is associated with the commercial site name that it received in the message from the access appliance.

The key regenerates the commercial site's cryptographic signature of the random sequence of letters and the transaction docket contained in the message received from the access appliance using the key's copy of the commercial site's secret number. The key compares the commercial site's cryptographic signature that it

received in the message from the access appliance with the cryptographic signature that it generated independently.

If the signatures do not match **45**, the key sends a message to the access appliance **46** that indicates that the commercial site message could not be authenticated. The key cannot perform any other function until it receives a message from a site that it can authenticate. The key maintains a count of consecutive failures to authenticate commercial sites. If there are more than a predefined number of consecutive failures the key disables itself permanently. If the signatures match, the key generates a cryptographic signature of the random letters received from the commercial site together with the transaction docket using the user's secret number that is stored in the key, a copy of which is contained in the user's record on the commercial site.

The key sends the user's cryptographic signature to the access appliance to indicate that the key has successfully authenticated the server message and the transaction docket **48**. The access appliance sends the user's cryptographic signature of the random letters and the transaction docket **43** to the commercial site. The commercial site retrieves the random letters and the transaction docket from the user's record and generates a cryptographic signature of them using its copy of the user's secret number. If the signature matches the signature that is received from the access appliance then the transaction is authenticated. The Website then executes the transaction **54**.

The user and peer will receive notifications from the Verifox server that the transaction has been verified and executed. All other transaction details are carried out directly between the user' s financial institution and the peer. No personal information whatsoever has to be transferred between the user and peer.

The same verification process is carried out each time a new transaction page is entered, or after chosen time intervals, in order to ensure that no unauthorized parties intervene in the buying process, however dynamic this process may be.

The current invention can also be used in other contexts where sharing of information is of a sensitive nature. For example, transfer of restricted technical

information, secret personal medical information, remote operation of software, secretive military information etc. may require highly secure authentication, which can be supplied by the current invention.

Another feature of the key is the disabling process, by which a key, which is used in an unauthorized way, can be automatically permanently disabled.

While the invention has been described with respect to a limited number of embodiments, it will be appreciated that many variations, modifications and other applications of the invention may be made.

WHAT IS CLAIMED IS:

1. A system for automatically cross-authenticating digital identities of information partners or transactional peers without transferring personal information between them, comprising:

   an active smart-key for storing personal information and processing identity verification, which can connect to various Internet enabled systems and devices;

   a server database for storing personal information and processing identity verification and communications in two separate processes, between the peer and the server, and between said smart key or said Internet enabled systems and devices and the server.

2. A system for automatically cross-authenticating digital identities of information partners or transactional peers without transferring personal information between them, according to the following steps:

   pre-registration at a licensed agent including giving over of personal and financial information and receiving of a personal security key device;

   dual authentication of both user and peer against said agent for all transactions or information transfers involving the system.

   automatic execution of said transaction after said authentication has been verified.

3. The system of claim 1, wherein the digital identities of all involved parties are verified every time a relevant new page or device is accessed.

4. The system of claim 1, wherein the active smart-key is a mobile hardware or even software based device with an internal mini-computer, including a central processing unit, read-only memory, random-access memory and EEPROM, that can be connected to any device supporting a USB, RS232, infrared wireless technology or any other relevant communications technology.

5. The system of claim 4, wherein said active smart-key can store, process and communicate encrypted information, using a trap door algorithm and a hash function.

6. The system of claim 4, wherein said active smart-key contains a fragile envelope, based on a shattering casing or a glass bead interior that can disable the device when being opened up.

7. The system of claim 1, wherein authentication is performed continuously without the need for the user to confirm, so that the system automatically matches between users, renewing the authentication on every new page where sensitive information can be transferred.

8. The system of claim 7, wherein the message starting each authentication process is random.

9. A method for automatically cross-authenticating digital identities of information partners or transactional peers without transferring personal information between them, according to the following steps:

pre-registration at a licensed agent including giving over of personal and financial information and receiving of a personal security key device;

dual authentication of both user and peer against said agent for all transactions or information transfers involving the system.

automatic execution of said transaction after said authentication has been verified.

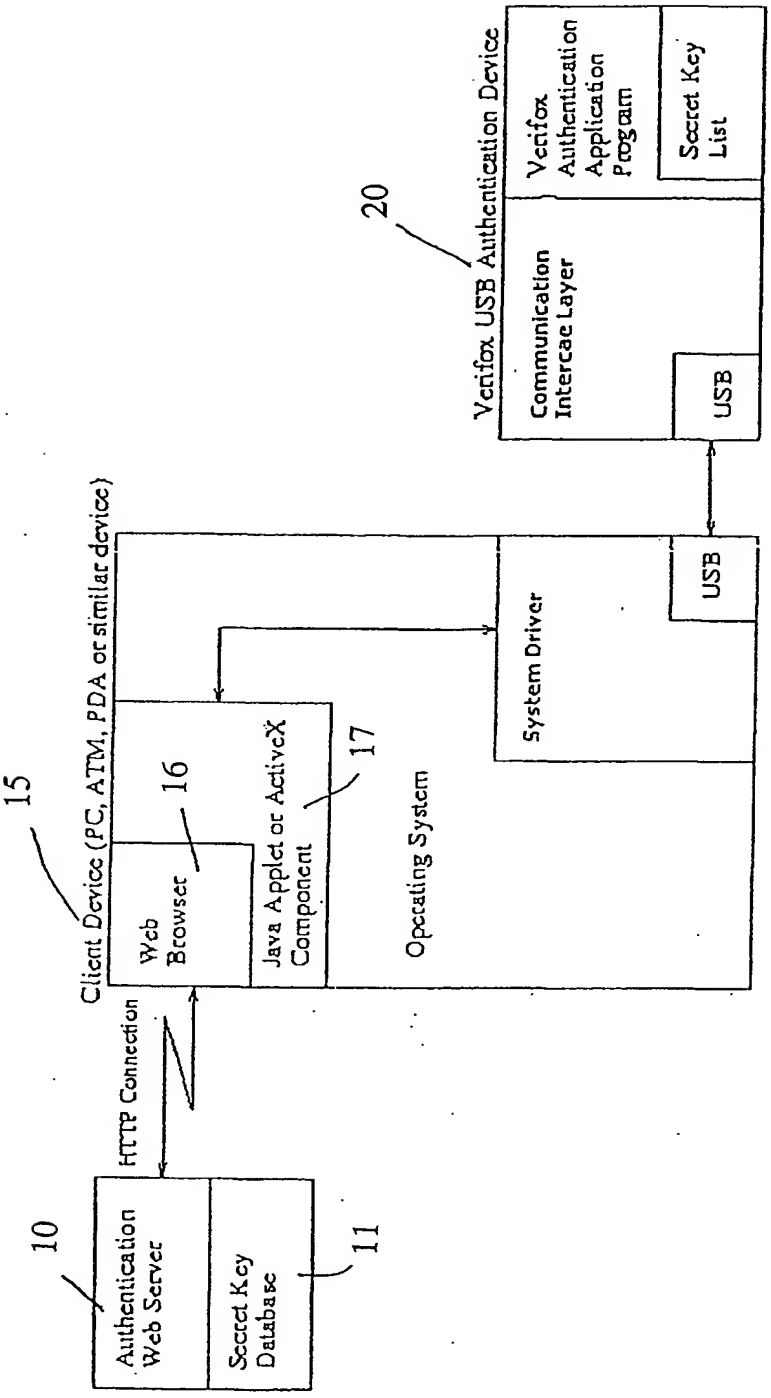
Verifox USB Authentication Device
Communication Intercae Layer
USB
Verifox Authentication Application Program
Secret Key List
20
Client Device (PC, ATM, PDA or similar device)
Web Browser
16
Java Applet or ActiveX Component
17
Operating System
System Driver
USB
15
HTTP Connection
Authentication Web Server
Secret Key Database
10
11

FIGURE 1

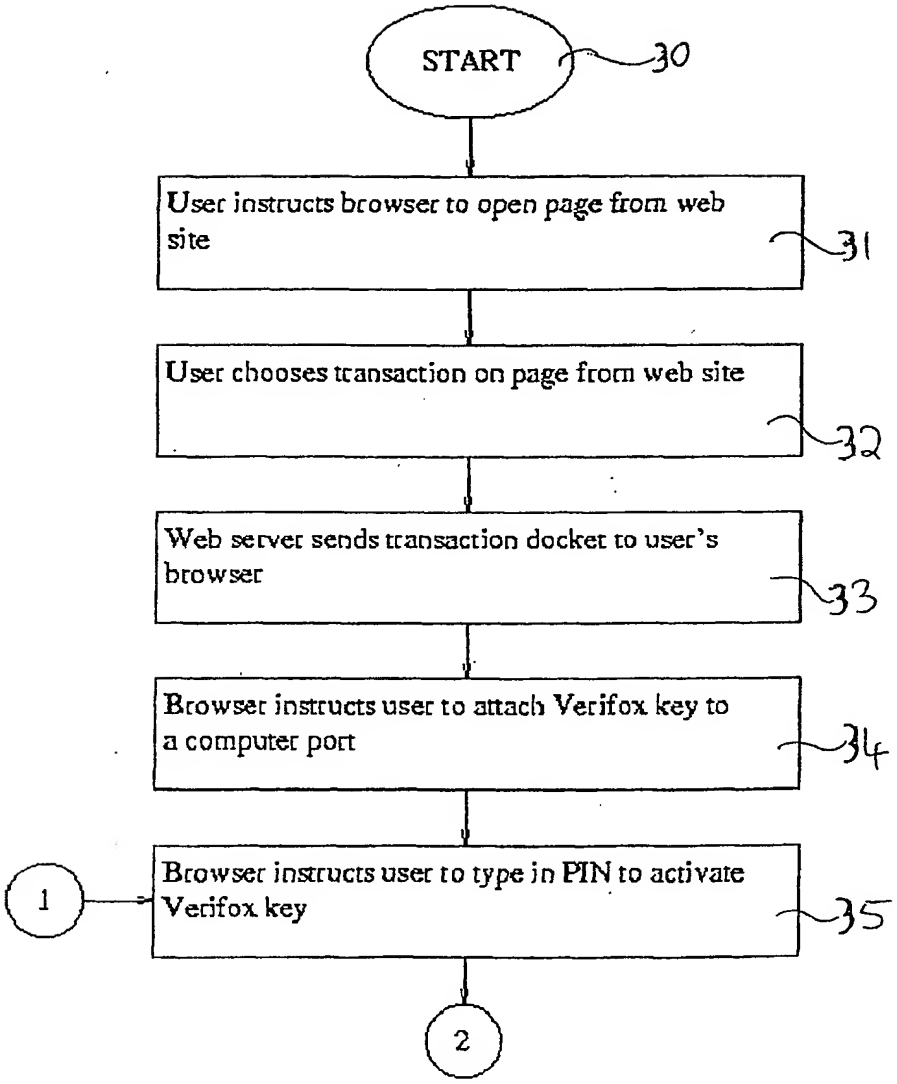
START
30
User instructs browser to open page from web site
31
User chooses transaction on page from web site
32
Web server sends transaction docket to user's browser
33
Browser instructs user to attach Verifox key to a computer port
34
1
Browser instructs user to type in PIN to activate Verifox key
35
2

FIGURE 2a

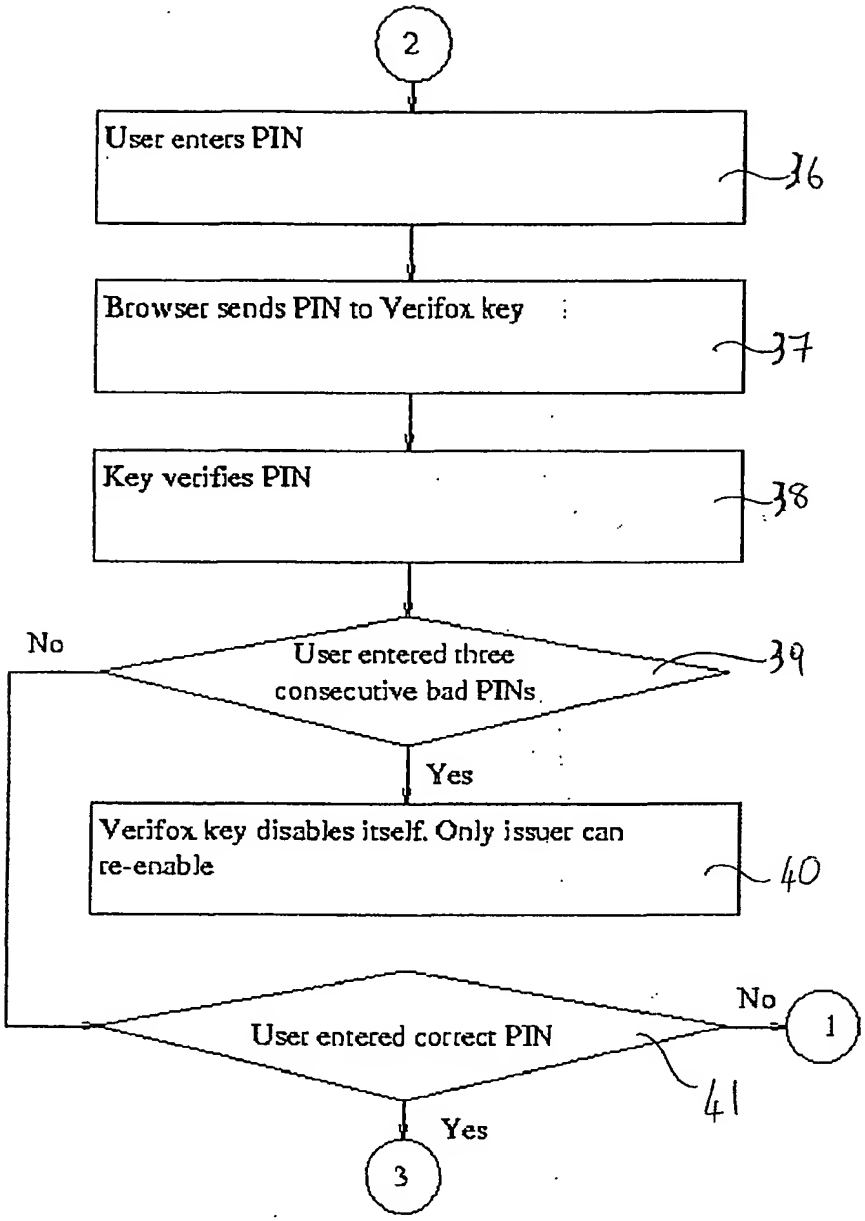
2
User enters PIN
36
Browser sends PIN to Verifox key
37
Key verifies PIN
38
No
User entered three consecutive bad PINs
39
Yes
Verifox key disables itself. Only issuer can re-enable
40
No
1
User entered correct PIN
41
Yes
3

FIGURE 2b

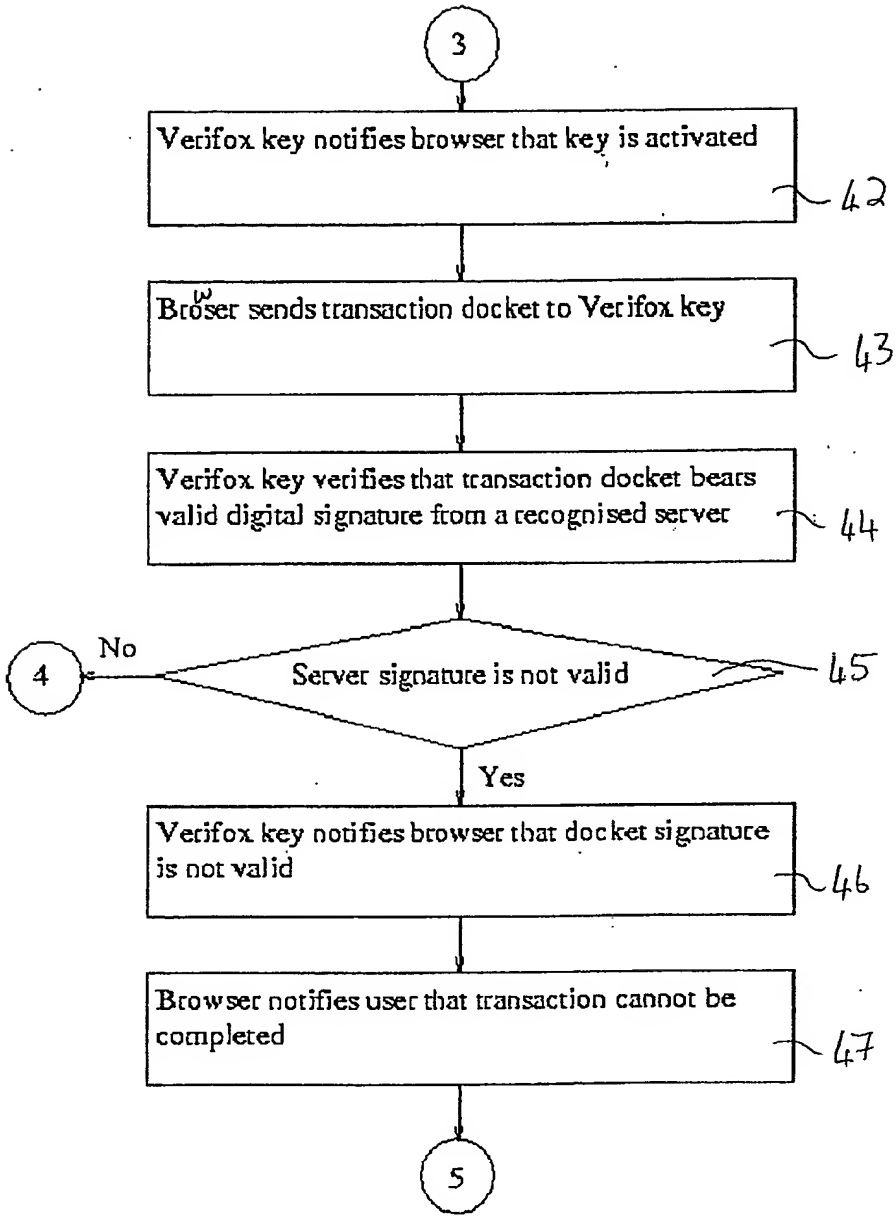
3
Verifox key notifies browser that key is activated
42
Browser sends transaction docket to Verifox key
43
Verifox key verifies that transaction docket bears valid digital signature from a recognised server
44
No
4
Server signature is not valid
45
Yes
Verifox key notifies browser that docket signature is not valid
46
Browser notifies user that transaction cannot be completed
47
5

FIGURE 2c

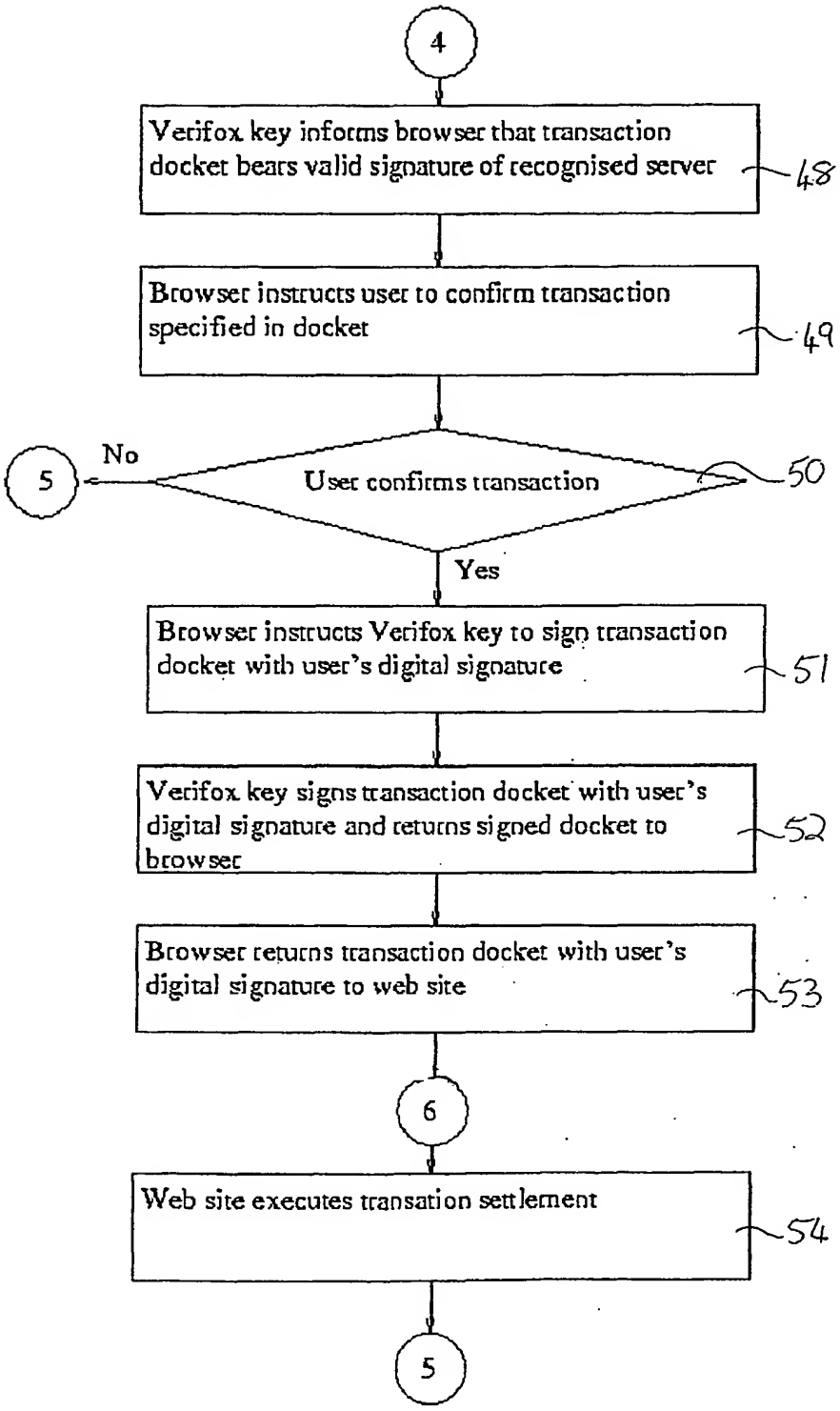
4
Verifox key informs browser that transaction docket bears valid signature of recognised server
48
Browser instructs user to confirm transaction specified in docket
49
No
5
User confirms transaction
50
Yes
Browser instructs Verifox key to sign transaction docket with user's digital signature
51
Verifox key signs transaction docket with user's digital signature and returns signed docket to browser
52
Browser returns transaction docket with user's digital signature to web site
53
6
Web site executes transation settlement
54
5

FIGURE 2d

INTERNATIONAL SEARCH REPORT

Inter: ɔnal application No.
PCT/IL01/00620

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/00; H04K 9/00
US CL : 713/159,168,169,172,185; 705/67,77,78
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/159,168,169,172,185; 705/67,77,78

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,778,071 A (CAPUTO et al.) 07 July 1998, col.6, lines 41-61, col.13, lines 4-13, col.16, lines 28-61.	1-9
Y	US 5,761,309 A (OHASHI et al.) 02 June 1998, col.5, lines 41-67, col.6, lines 1-12, col.8, lines 5-12.	1-9
A	US 6,044,470 A (KURIYAMA) 28 March 2000, col.7, lines 4-18, col.,8 lines 49-65.	1-9
A	US 5,623,637 A (JONES et al.) 22 April 1997, col.2,lines 44-50, col.8, lines 52-67.	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 08 NOVEMBER 2001	Date of mailing of the international search report 14 DEC 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 305-0042

Form PCT/ISA/210 (second sheet) (July 1998)*

B.. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

STN,EAST
search terms: token,smart card,IC card,intelligent token,portable device,cellular phone,laptop,notebook,smart key,memory,authentication,verify,check,password,ID,PIN,Internet